

AO93 Search and Seizure Warrant

SEALED

ORIGINAL
UNITED STATES DISTRICT COURT
for the
District of Arizona

In the Matter of the Search of
Safety Deposit Box #821 Located at JP Morgan Chase Bank,
Branch #0601.

Case No. 22-9302 MB
(Filed Under Seal)

SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of Arizona:

As further described in Attachment A-3.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal:

As set forth in Attachment B.

YOU ARE COMMANDED to execute this warrant on or before 9/5/2022 *(not to exceed 14 days)*
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night as I find reasonable cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to any United States Magistrate Judge on criminal duty in the District of Arizona.

☐ I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized ☐ for 30 days *(not to exceed 30)* ☐ until, the facts justifying, the later specific date of _____.

Date and time issued: 8/22/2022@8:06pm

E. Willett
Judge's signature

City and state: Phoenix, Arizona

Honorable Eileen S. Willett, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A-3

LOCATION 2 – J.P. MORGAN CHASE BANK

SAFETY DEPOSIT BOX



Safety Deposit Box number #821 located at J.P. Morgan Chase Bank, Branch #0601, 3502 West Bell Road, Glendale, AZ 85308.

ATTACHMENT B
(RESIDENCE, VEHICLE, SAFETY DEPOSIT BOX, PHONE, AND ELECTRONIC
STORAGE MEDIA)

Property to be seized

1. All items relating to violations of 18 U.S.C. § 1958 and 18 U.S.C. § 373, involving **ALI JOSEPH**, and others known and unknown, occurring between July 4, 2021 and present, including:

- a. Records and information relating to communications, including emails, text messages, direct messages, voicemails, encrypted communications and associated meta data regarding child custody issues with or about the VICTIM, listed in the Search Warrant Affidavit;
- b. Records and information relating to communications, including emails, text messages, direct messages, voicemails, encrypted communications and associated meta data regarding disagreements with the VICTIM regarding raising of ALI JOSEPH's children;
- c. Records and information including photographs of the VICTIM and any documents reflecting the name, address, vehicle description, or vehicle license plate of the VICTIM;
- d. Records and information relating to communications, including emails, text messages, direct messages, voicemails, encrypted communications and associated meta data discussing causing harm to the VICTIM;
- e. Records and information relating to communications, including emails, text messages, direct messages, voicemails, encrypted communications and associated meta data regarding murder-for-hire plan targeting the VICTIM;

- f. Records and information, including papers, writings, documents, and data either to, from, or found in the possession of ALI JOSEPH regarding a murder-for-hire plan targeting the VICTIM;
- g. Records and information relating to motive for the murder-for-hire plan targeting the VICTIM, including any articulated grievances with the VICTIM;
- h. Records and information relating to online searches of hiring an individual to commit murder, committing murder with a vehicle, committing murder by stabbing, death, causing accidental deaths, muggings, and robberies;
- i. Records and information showing any descriptions, plans, photographs, and/or writings related to threats or violence against the VICTIM;
- j. Records and information reflecting the hiring or payment to any person for services related to locating, threatening, or harming the VICTIM;
- k. Records and information relating to financial transactions for payment to any person for services related to locating, threatening, or harming the VICTIM;
- l. Records and information depicting photos or videos of surveillance of the VICTIM;
- m. Records and information relating to international travel by ALI JOSEPH and/or his children;
- n. All cellular telephones maintained, controlled, utilized, or possessed by ALI JOSEPH, and/or located at the property to be searched, to the extent that this not addressed below; and
- o. Computers, devices and electronic storage media used as a means to commit the violations described above.

2. For any computer or electronic storage medium whose seizure is otherwise authorized by these warrants, and any computer or electronic storage medium that contains or in which is stored records or information that is otherwise called for by these warrants (hereinafter, "COMPUTER"):

- a. Evidence of who used, owned, or controlled the COMPUTER at the time the things described in these warrants were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. Evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. Evidence of the lack of such malicious software;
- d. Evidence indicating how and when the computer was accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;
- e. Evidence indicating the computer user’s state of mind as it relates to the crimes under investigation;
- f. Evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- g. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- h. Evidence of the times the COMPUTER was used;
- i. Passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- j. Documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- k. Records of or information about Internet Protocol addresses used by the COMPUTER;

- l. Records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and
- m. Contextual information necessary to understand the evidence described in this attachment.

3. Evidence of user attribution showing who used or owned the Device at the time the things described in these warrants were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history;

4. Records evidencing the use of the Internet Protocol addresses to communicate with others regarding child custody issues, locating, threatening, or harming the VICTIM, including:

- a. records of Internet Protocol addresses used; and
- b. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

5. Routers, modems, and network equipment used to connect computers to the internet.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

The term "computer" includes all types of electronic, magnetic, optical, electrochemical, or other high speed data processing devices performing logical, arithmetic, or storage functions,

including desktop computers, notebook computers, mobile phones, tablets, server computers, and network hardware.

The term “storage medium” includes any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

During the execution of the search of the RESIDENCE, the VEHICLE, the SAFETY DEPOSIT BOX and the PHONE described in Attachments A-1, A-2, A-3, and A-4, law enforcement personnel are authorized to (1) press or swipe the fingers (including thumbs) of any individual, who is found at the RESIDENCE, the VEHICLE, and the SAFETY DEPOSIT BOX and reasonably believed by law enforcement to be a user of a device found at the premises, to the fingerprint scanner of the device; (2) hold a device found at the premises in front of the face those same individuals and activate the facial recognition feature, for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant.

These warrants authorize a review of electronic storage media and electronically stored information seized or copied pursuant to these warrants in order to locate evidence, fruits, and instrumentalities described in these warrants. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to these warrants, the FBI may deliver a complete copy of the seized or copied electronic data to the custody and control of attorneys for the government and their support staff for their independent review.

AO 93 (Rev. 01/09) Search and Seizure Warrant (Page 2)

RETURN

Case No.:	Date and Time Warrant Executed:	Copy of warrant and inventory left with:
22-9302 MB	8-24-2022 9:00 AM	N/A

Inventory Made in the Presence of:

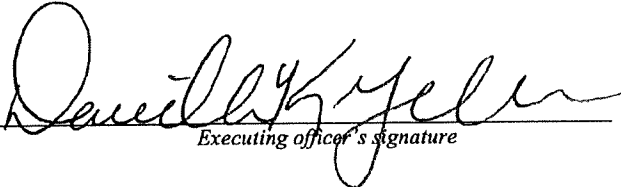
Bruce Keefer

Inventory of the property taken and name of any person(s) seized:

None - wrong address
not served**CERTIFICATION**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: 8/29/2022


Executing officer's signatureDanielle Williams, Special Agent FBI
Printed name and title